REMARKS

Claims 1, 2, 5, 7, 8, 11, and 13-15 are currently pending. Claims 3, 4, 6, 9, 10, and 12 have been cancelled. Claims 1 and 7 have been amended. Claims 14 and 15 have been added. The support for the amendment of claim 1 is found in original claims 1, 3, 4, and 6, and Figure 2. The support for the amendment of claim 7 is found in original claims 9, 10, and 12, and Figure 2. The support for new claims 14 and 15 is found in originally claims 1 and 7 and page 7, lines 6-14, of Applicant's specification. It is respectfully submitted that no new matter has been added.

The specification has been amended for clarification. Changes to the specification include replacing the two paragraphs according to the response of July 29, 2005, in the summary of the invention with two paragraphs that describe in detail the claimed subject matter that had previously only referred to claims by number. It is respectfully submitted that no new matter has been added.

The Patent Office rejected claims 3, 4, 9, and 10 under 35 U.S.C. § 112, 2nd Paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 3, 4, 9, and 10 were rejected under 35 U.S.C. § 112, 2nd Paragraph, as having insufficient antecedent basis for the limitation "the internet." Applicant still asserts there is no ambiguity as there is only one internet and that the internet is a well defined term, but to facilitate prosecution, has amended the claims to recite "an internet" in the first instance of this term. Thus, it is respectfully requested that the Patent Office withdraw its rejection of the subject matter of claims 3, 4, 9, and 10, now incorporated into claims 1 and 7, under 35 U.S.C. § 112, 2nd Paragraph.

The Patent Office rejected claims 1, 2, 5, 7, 8, 11, and 13 under 35 U.S.C. 103(a) as being unpatentable over McManis, "System and Method for Protecting Use of Dynamically Linked Executable Modules," U.S. Patent No. 5,757,914. As claims 3, 4, 9, and 10 have been incorporated into claims 1 and 7, Menezes et al., Handbook of Applied Cryptography, is also discussed.

Claim 1 recites "wherein, if a public key cannot be obtained via an internet site of a virtual machine provider, the digital signature key is a hidden public key internal to the loader program and, if a public key can be obtained via the internet site of the virtual machine provider, the digital signature key is the public key obtained via the internet site of the virtual machine provider" and "wherein the loader program is arranged to verify and selectively load the primary library file by comparing the obtained digital signature key with the digital signature of the primary library file, the primary library file being further arranged to subsequently verify and selectively load the plurality of secondary files by calling the loader program to compare the obtained digital signature key with the digital signature of each of the plurality of secondary files, wherein the computer software installation is a virtual machine installation." Menezes, as will be discussed below, fails to teach or fairly suggest these claim limitations.

Claim 7 recites "if a public key is available from an internet site of a virtual machine provider, using the public key as a digital signature key; if a public is not available from the internet site of the virtual machine provider, using a hidden key as the digital signature key; using the loader program to verify the authenticity of a digital signature incorporated in a primary library file by comparing said digital signature with the digital signature key; selectively loading the primary library file in dependence upon the successful verification of its digital signature" and "selectively loading the plurality of secondary files in dependence upon the successful verification of their digital signatures, wherein the computer software installation is a virtual machine installation." Menezes, as will be discussed below, fails to teach or fairly suggest these claim limitations.

Applicant has identified problems with the current art; e.g., a hacker can alter the behavior of the JVM outside the JVM environment to under the whole Java security model (page 1, line 25, through page 2, line 4) such as by disabling the security code or by inserting destructive routines into the core of the JVM (page 2, lines 13-17). The present invention provides a scheme for verification of the authenticity of a JVM using digital signatures and offers advantages. These advantages include 1) enhanced security of the JVM, 2) greater user confidence in the correct function of Java applications, and 3) improved detection of incorrect or damaged JVM installations (page 9, line 20, through page 10, line 2, of Applicant's specification).

The Patent Office asserted (Page 3, lines 14-19, of the Office Action mailed July 1, 2005) "McManis discloses: *a primary library file having a digital signature* (McManis, col. 1, line 65 – col. 2, line 11; col. 1, lines 48-63); *a loader program arranged to obtain a digital signature key* *and further arranged to load the primary library file* (McManis, fig. 1, elems. 110, 112; col. 2, lines 22-37, 40-43). The verifier is a "loader program" as it enables the loading of each program module, including the primary program module. *And a plurality of secondary files arranged to be referenced by the primary library file, each of the plurality of secondary files having a digital signature* (McManis, fig. 1, elems. 116, 118, 120; col. 2, lines 1, 2; col. 3, lines 17-21)."

The claimed invention recites "wherein the loader program is arranged to verify and selectively load the primary library file by comparing the obtained digital signature key with the digital signature of the primary library file" and "selectively loading the plurality of secondary files in dependence upon the successful verification of their digital signatures," whereas McManis is limited to the mutual verification by two applications. Despite the Patent Office's assertion, McManis's verifier is not a "loader program." Just because a software module is able to verify the authenticity of an application does not mean that it will also load such application.

The Patent Office (page 6, lines 1-6, of the Office Action mailed July 1, 2005) asserts "McManis shows the operation of his system in a slice of time (McManis, col. 2, lines 53-55). He does not disclose the details regarding the initialization of his system, but instead shows how his loader program enables the loading of the primary and secondary files via the verification of digital signatures. Consequently, McManis does not disclose an initial digital signature verification of the primary file by the loader program, an initial loading of the primary file by the loader program".

Applicant asserts that McManis discloses a verifier that is usable by a calling application and a called application, but does not disclose a loader arranged to obtain a digital signature key and further arranged to load the primary library file, as claimed. Since McManis is concerned with preventing use or export of certain cryptographic routines, trade secret functions, and functions protected by contract (column 1, lines 37-63), McManis is not concerned with the basic software but with certain called routines and so it not concerned with the initial loading of a base application, such as a JVM.

The Patent Office (page 4, lines 3-11, of the Final Office Action mailed October 21, 2005) further asserts "However, McManis discloses that every file, including the primary files, contains a digital signature and that the digital signature is necessary to verify the authenticity of every called file before that file is loaded (McManis, col. 1, line 65 – col. 2, line 44). It would have been obvious to one of ordinary skill in the art to arrange, at the time of initialization, for the loader program to initially verify the digital signature of the primary file and initially load the primary file. This would have been obvious because one of ordinary skill in the art would have been motivated to verify the authenticity of the primary file, as taught by McManis, when the primary file is initially loaded – so as to protect the system's integrity at all times."

Applicant, in response to the above paragraph, again asserts that McManis does not disclose loading and does not disclose loading as being part of the verification process. McManis does not disclose that the primary file is verified by a loading program. McManis discloses a mutual verification process where a calling application verifies the digital signature of a called application and the called application verifies the digital signature of the calling application (e.g., Figure 2). The first problem McManis addresses concerns the isolation of cryptographic routines to prevent the export of sensitive technology (column 1, lines 37-57) so McManis would not be directed to the verification of a basic Java virtual machine, but at cryptographic routines that might be called by the JVM. The second problem McManis addresses concerns the situation where there is a desire to limit or prevent use of dynamically linkable modules so as to protect trade secrets or provide protection for contractual reasons so McManis would also not be directed to verification of a basic Java virtual machine.

Claim 1 has been amended to incorporate the limitations of claims 3 and 4 in accordance with the method shown in Figure 2. Claim 7 has been amended to incorporate the limitations of claim 9 and 10 in accordance with the method shown in Figure 2.

The limitations of canceled claims 3 and 9, now incorporated into claims 1 and 7, are addressed.

The Patent Office asserted (page 6, line 11, through page 7, line 2, of the Final Office Action mailed October 21, 2005)

> Regarding claim 3, the modification of McManis discloses the use of a public key as a digital signature key (McManis, col. 3, lines 38-50). He does not disclose that the public key is obtained from the internet.
>
> Menezes et al. discloses the key management techniques used to share keying material (Menezes et al., pages 543, 544). In public-key systems, entities requiring public keys obtain the public keys via an internet ("inter network") of certification authorities, key servers, and key management facilities (Menezes et al., pages 548-550).
>
> It would have been obvious to one of ordinary skill in the art to employ the

> method Menezes et al. for obtaining public keys via an internet with the system of McManis for using a public digital signature key. This would have been obvious because one of ordinary skill in the art would have been motivated to efficiently utilize system resources by having the public key be obtained from a remote source instead of the program modules themselves generating the public/ private key pairs.

Menezes is concerned with key management techniques and does not disclose a loader arranged to obtain a digital signature key and further arranged to load the primary library file, as claimed. Since McManis is concerned with preventing use or export of certain cryptographic routines, trade secret functions, and functions protected by contract (column 1, lines 37-63), McManis is not concerned with the basic software but with certain called routines and so it not concerned with the initial loading of a base application, such as a JVM.

The limitations of canceled claims 4 and 10, now incorporated into claims 1 and 7, are addressed.

The Patent Office asserted (page 7, lines 4-12, of the Final Office Action mailed October 21, 2005)

> Regarding claim 4, the combination of McManis and Menezes et al. discloses: *the digital signature key being a hidden public key internal to the loader program, the loader program being arranged to use the hidden public key the event that a public key cannot be obtained via the internet* (McManis, col. 4, lines 7-53). The combination of McManis and Menezes et al. shows that public keys used for digital signature generation would be obtained from an internet. The loader program obtains the public key and inherently stores the key internally (as would be required in order to perform the processing of the digital signatures), thus using the obtained key even if it couldn't be obtained by the loader program from an internet.

Both McManis and Menezes are silent regarding a hidden public key and neither disclose or suggest the limitation "the loader program being arranged to use the hidden public key in the event that a public key cannot be obtained from the internet". Furthermore, McManis' discloses an embedded public key, but does not suggest or disclose both a hidden public key and a public key obtained via the internet. Thus, claims 1 and 7 are allowable over the prior art of record.

The limitations of canceled claims 6 and 12, now incorporated into claims 1 and 7, are addressed.

The Patent Office asserts (page 5, lines 12-21, of the Final Office Action, mailed October

21, 2005) "Regarding claim 6, the modification of McManis does not disclose that the system is a Java Virtual Machine installation. However, the system of McManis, assigned to Sun Microsystems, Inc., is disclosed as being operable on "virtually any type of computer", including architecturally distinct systems such as Sun workstations, IBM compatible computers, and Macintosh computers. It would have been obvious to one of ordinary skill in the art, based upon logical reasoning, to employ a virtual machine installation such as Java in the system of McManis. This would have been obvious because one of ordinary skill in the art would have logically recognized that a virtual machine installation such as Java would allow the system of McManis to be employed on such a diverse and distinct set of architectures."

Applicant is concerned with providing security for the installation of a Java Virtual Machine (page 3, lines 4-6, and page 4, lines 22-27, of Applicant's specification) and notes that the prior art includes virtual machine enhanced security models that does not divulge sensitive information (page 1, lines 12-23, of Applicant's specification). Applicant asserts that McManis does not disclose or fairly suggest a Virtual Machine software installation, as found in claims 1 and 7.

In view of the above, allowance of claims 1, 2, 5, 7, 8, 11, and 13 is respectfully urged.

Claim 2 recites "wherein after successful verification and selective loading of the at least one secondary file, the at least one secondary file is arranged to manage the verification and selective loading of the at least one tertiary file."

Claim 8 recites "after successful verification and selective loading of the at least one secondary file; using the at least one secondary file to manage the verification and selective loading of the at least one tertiary file."

The Patent Office asserts "Regarding claim 2, the modification of McManis discloses: *the plurality of files including at least one tertiary file referenced by at least one secondary file of the plurality of secondary files, wherein after successful verification and selective loading of the at least one secondary file, the at least one secondary file is arranged to manage the verification an selective loading of the at least one tertiary file* (McManis, fig. 1, elems. 118, 120; col. 3, lines 12-21, 30-37). McManis discloses that each file can contain a plurality of procedure calls to other files, thus a secondary file may call a tertiary file."

Applicant asserts that McManis does not disclose or suggest the limitation "wherein after successful verification and selective loading of one of the at least one secondary file, the at least one secondary file is arranged to manage the verification and selective loading of the at least one tertiary file." Even if column 3, lines 12-21 and 30-37, figure 1, and elements 118 and 120 of McManis could be construed to as a suggestion for a tertiary file, McManis does not disclose or suggest that "at least one secondary file is arranged to manage the verification and selective loading of the at least one tertiary file." Thus, it is respectfully submitted that claims 2-5, 8 and 11 are allowable for this additional reason.

Claim 5 recites "comprising at least one administrator-configurable file" and "wherein the loader program is further arranged to verify the digital signature of the at least one administrator-configurable file using the private key."

Claim 11 recites "comprising at least one administrator-configurable file" and "wherein the loader program is further arranged to verify and selectively load the digital signature of the at least one administrator-configurable file using the private key."

The Patent Office asserted (page 7, lines 4-13 of the Final Office Action mailed October 21, 2005) "Regarding claim 5, the modification of McManis discloses that all files contain digital signatures so that they may be verified with a digital signature key (McManis, col. 2, lines 22-37). McManis further discloses that verifiable files may contain a number of portions, including a methods portion and a data portion. Each portion is verified by a separate digital signature (McManis, col. 4, lines 54-67). Thus, McManis discloses the digital signature key used to verify the file as being a combination of keys. These verifiable files are often authored, maintained, or updated ("administered") by others ("administrators"), which is why they are linked dynamically during program execution (McManis, col. 1, lines 10-27). Thus, the modification of McManis discloses at least one of the files as being an administrator configurable file."

Applicant asserts that McManis contains no teaching or suggestion of the limitation "wherein the loader program is further arranged to verify the digital signature of the at least one administrator-configurable file using the private key" and does not disclose an "administrator-configurable file." Thus, it is respectfully submitted that claims 5 and 11 are allowable over the prior art of record.

The Patent Office rejected claims 3, 4, 9, and 10 under 35 U.S.C. 103(a) as being unpatentable over McManis, "System and Method for Protecting Use of Dynamically Linked

Executable Modules," U.S. Patent No. 5,7575,914, in view of Menezes et al., Handbook of Applied Cryptography.

Please see the discussion above with respect to amended claims 1 and 7.

Regarding the Patent Office's Response to Arguments starting on page 7, line 17, of the Final Office Action mailed October 21, 2005.

(i) Applicant maintains that there is only one Internet. However, to facilitate prosecution, Applicant has amended the claims to refer to an internet site.

(ii) McManis does not disclose the verifier as a "loader program."

(iii) Applicant recognizes that security is providing for loading software modules in the current art, but has recognized a problem that current known methods for installing virtual machines are vulnerable (see Applicant's background of the invention). Applicant provides a solution to this identified problem.

(iv) The limitation in question concerns "tertiary files," a feature not addressed on page 10, line 19, through page 11, line 7, of the Final Office Action, mailed October 21, 2005.

(v) Regarding the remark about compliance with 37 CFR 1.111(b), Applicant has bolded text in claims 5 and 11 that Applicant believes is allowable subject matter with respect to the prior art of record.

(vi) None of the prior art references are believed to disclose or fairly suggest a Virtual Machine software installation.

(vii) McManis is not concerned with virtual machine installations, but is directed to called routines. Applicant does recite a virtual machine in the claims. Applicant notes that remark (vii) relates to claims 3 and 9. The subject matter of these claims concerned the use the type of key to be used as the digital signature key, and in conjunction with the limitations of their corresponding base and intervening claims would at least present a patentable combination of features.

(viii) None of the prior art of record, alone or in combination, makes obvious the limitations of claims 4 and 10, which have now been incorporated into the independent claims.

The Examiner is respectfully requested to reconsider and remove the rejections of the claims 1, 2, 5, 7, 8, 11, and 13 under 35 U.S.C. 103(a) based on McManis, U.S. Patent No. 5,757,914, alone or in combination with Menezes et al., Handbook of Applied Cryptography, and to allow all of the pending claims 1, 2, 5, 7, 8, 11, and 13 as now presented for examination. An early notification of the allowability of claims 1, 2, 5, 7, 8, 11, and 13 is earnestly solicited.

Respectfully submitted:

Walter J. Malinowski December 21, 2005

Walter J. Malinowski Date

Reg. No.: 43,423

Customer No.: 29683

HARRINGTON & SMITH, LLP
4 Research Drive
Shelton, CT 06484-6212

Telephone: (203)925-9400, extension 19
Facsimile: (203)944-0245
email: wmalinowski@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

December 21, 2005

Date Name of Person Making Deposit